Security Requirements for Systems Hosted in Managed Care or Customer Managed Environments

A. Standards

Listed below are two standard requirements relate specifically to SB 954 projects constructed in the Customer Managed Domain environment only.

1. Projects that are classified as SB 954 projects and are constructed in the customer managed domain environment must follow the COEMS process to gain access to the data center. Please refer to the Customer Managed Domain Facility Access.doc.

2. Production documentation for turnover to DTS Security staff. This includes but is not limited to
   a) Service Level Agreements;
   b) System requirements;
   c) Network configuration diagrams and settings (i.e.: firewall ports & protocols);
   d) Identification of all system administrator logon locations;
   e) Hardware manuals.

Listed below are ten standard requirements they relate to ALL projects in both the Customer Managed Domain and hosted environments.

1. Network Architectures: DTS Security Management Division prefers to manage the below three types of architectures:
   a) **DMZ**/*Firewall with Application Ports*/**Application Tier**/*Firewall with DB Ports*/**Database Tier**
   b) Proxy/*Firewall with Web Ports*/**DMZ & Application Tier**/*Firewall with DB Ports*/**Database Tier**
   c) Proxy/**DMZ & Application & DB Tier ONLY for z/OS systems**

2. Data repositories containing Confidential or Sensitive data must reside on a firewalled VLAN separate from the DMZ & Application tier(s).

3. No Database Management Systems are allowed on a public Internet accessible network.

4. Authentication devices cannot reside in the DMZ. (i.e.: Domain Controllers, Active Directories.

5. Systems that involve credit card transactions must adhere to established PCI standards. The customer or vendor responsible for building/designing the system must provide DTS with:
    a) Proof that they are PCI certified;
    b) Proof that the credit card processor being used is a certified processor; and
    c) Documentation proving the systems compliance with PCI.

6. All firewall ports are closed by default for testing, development or production environments; instead, request specific ports or a range of ports as early as possible.

7. Firewall port and access control list request changes should be made via a Service Request with the Firewall and Access List Request Form (DTS 363) attached.

8. Customer ISO approval is required on all service and change requests involving:
    a) Consulting for security or operational recovery;
    b) Confidential or sensitive data;
    c) Dial-in lines;
    d) Non-state users accessing the system/data; and/or
    e) Firewall port or access list requests.

9. Intrusion Prevention Systems are active at the DTS perimeter. IPSs are not host-based.

10. Vulnerability scans of production servers take place regularly. Reports can be shared with customers upon request.

11. System data must be classified by the customer per the State Administrative Manual (SAM) section 4841.3 and disclosed to DTS staff.

12. Systems cannot allow direct public access to the application and database tiers.

B. Recommendations

Listed below are recommendations for both the Customer Managed Domain and hosted environments.

1. Show where the system is compliant with industry standard requirements (i.e.: PCI, HIPAA) up front instead of during implementation.

2. Confidential and sensitive information should be encrypted in transit and at rest.

3. Provide notice to DTS prior to system patching and/or maintenance so that technicians are aware and do not take unnecessary actions. This applies to all environments. (i.e.: test/development/training/pre-production/ production.)

4. Provide detailed network architecture diagrams, including ports, protocols, hardware placement, and data flow, prior to procurement or implementation of any DTS housed environment. The earlier the better so that security concerns can be brought to light mitigating any delay to the project schedule.

C. Glossary

Listed below is DTS Security Management Division's interpretation of some common industry/IT terms.

Industry Definition	**DTS Term**
Internet facing web tier	Demilitarized Zone (DMZ)
World Wide Web	Public Facing
n-tiered architecture tiers or layers	Tiers
Inter Agency Internet	CSGNet

D. Acknowledgment

Please sign below indicating that you have read and understand the DTS business requirements as indicated above.	
_____ **Customer ISO Signature**	_____ **Date**
_____ **Vendor/Contractor Signature**	_____ **Date**